Application Serial Number: 09/498,716
1.111 Amendment dated March 10, 2004
Reply to Office Action dated December 10, 2003

Attorney Docket Number: 0225-4188

REMARKS

The above Amendment and the following remarks are responsive to the Office Action dated December 10, 2003. The Applicant requests entry of this Amendment, favorable reconsideration of this case, and early issuance of a Notice of Allowance.

Status of the Claims

Upon entry of this Amendment, the Applicants have rewritten claims 25–26, 32–34, 37, 40–42, 48–50, and 56. Thus, claims 25–56 are pending in the application. Claims 25, 33, 41, and 49 are independent claims.

Response to the Rejections under 35 U.S.C. § 112 (second paragraph)

The Examiner rejected claims 25–56 under 35 U.S.C. § 112, second paragraph, as being indefinite in that they fail to point out what is included or excluded by the claim language. The Applicants respectfully traverse these rejections.

The Examiner indicates that claims 25, 33, 41, and 49 are unclear as to how the limitations teach the derivation of a public key. In response, the Applicants have rewritten claims 25, 33, 41, and 49 to clarify the limitations of the claims. Claims 25, 33, 41, and 49, as presently claimed, clarify the derivation of a public key by adding the limitation "computing the public key as a function of p, q, and B". The Applicants assert that the specification provides proper support for this amendment to claims 25, 33, 41, and 49 on page 7, lines 1–13 and with the disclosure of Figure 4.

The Examiner further indicates that in claims 32, 40, 48, and 56 the phrase "and related schemes" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. In response, the Applicants have rewritten claims 32, 40, 48, and 56 to clarify the limitations of the claims. Claims 32, 40, 48, and 56, as presently

Application Serial Number: 09/498,716
1.111 Amendment dated March 10, 2004
Reply to Office Action dated December 10, 2003

Attorney Docket Number: 0225-4188

claimed, clarified the limitations of the claim by replacing the phrase "and related schemes" with "key exchange, such as a Diffie-Hellman key exchange, using the public key". The Applicants assert that the specification provides proper support for this amendment to claims 32, 40, 48, and 56 from page 23, line 6 to page 24, line 28 and with the disclosures of Figures 8 and 9.

The Examiner further indicates that in claim 37 the meaning of the phrase "the public ken" is unclear. In response, the Applicants have rewritten claim 37 to clarify the limitations of the claims. Claim 37, as presently claimed, clarified the limitations of the claim by replacing the phrase "the public ken" with "the public key". The Applicants assert that this was merely a typographical error.

The Examiner further indicates that in claim 49 the application of the claimed business is unclear. In response, the Applicants have rewritten claim 49 to clarify the limitations of the claims. Claim 49, as presently claimed, clarified the application of the claimed business, by adding to the preamble that the business method is "for a cryptosystem resident in a device that includes a memory". The Applicants assert that the specification provides proper support for this amendment to claim 49 from page 5, line 7 to page 6, line 36 and with the disclosures of Figures 1, 2, and 3.

For the reasons stated above, the Applicants believe that claims 25, 32–33, 37, 40–41, 48–49, and 56, as presently claimed, are allowable because these claims are definite, particularly point out and distinctly claim the subject matter that the Applicants regard and the invention, and have proper antecedent basis. Thus, the Applicants believe that the Examiner should withdraw these rejections as to claims 25, 32–33, 37, 40–41, 48–49, and 56.

Claims 26–32, 34–40, 42–48, and 50–56 depend from independent claim 25, 33, 41, or 49. For the previously stated reasons, independent claims 25, 33, 41, and 49 are allowable.

48807 v1

Since any claim that depends from an allowable independent claim is also allowable, the Applicants also believe that the Examiner should withdraw these rejections as to dependent claims 26–32, 34–40, 42–48, and 50–56.

Response to the Rejections under 35 U.S.C. § 101

The Examiner rejected claims 25–56 as reciting non-statutory subject matter. The Applicants respectfully traverse these rejections.

The Examiner indicates that the claimed invention teaches the mathematical manipulation of an abstract idea and has no tangible output. Independent claims 25, 33, 41, and 49, as presently claimed, recite "a cryptosystem resident in a device that includes a memory". Furthermore, independent claims 25, 33, 41, and 49, as presently claimed, recite "computing the public key as a function of p, q, and B". Thus, the Applicants assert that the Examiner should withdraw this rejection because independent claims 25, 33, 41, and 49, as presently claimed, include limitations that are directed to statutory subject matter and produce a public key as tangible output.

Claims 26–32, 34–40, 42–48, and 50–56 depend from independent claim 25, 33, 41, or 49. For the previously stated reasons, independent claims 25, 33, 41, and 49 are allowable. Since any claim that depends from an allowable independent claim is also allowable, the Applicants also believe that the Examiner should withdraw these rejections as to dependent claims 26–32, 34–40, 42–48, and 50–56.

Response to the Rejections under 35 U.S.C. § 103(a)

The Examiner rejected claims 25–56 under 35 U.S.C. § 103(a) as being unpatentable over ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory 31(4), 1985 (hereinafter "ElGamal"), in view of

48807 v1

Application Serial Number: 09/498,716
1.111 Amendment dated March 10, 2004
Reply to Office Action dated December 10, 2003

Attorney Docket Number: 0225-4188

Brouwer et al., "Doing More with Fewer Bits", Advances in Cryptology – Asiacrypt '99, pp. 321–332 (hereinafter "Brouwer"), and further in view of Lidl et al., Introduction to Finite Fields and their Applications", 1986, pp. 50–55 (hereinafter "Lidl"). The Applicants respectfully traverse this rejection.

ELGAMAL

ElGamal discloses a new signature scheme together with an implementation of the Diffie-Hellman key distribution scheme that achieves a public key cryptosystem. ElGamal further discloses that the security of both systems rely on the difficulty of computing discrete logarithms over finite fields.

BROUWER

Brouwer discloses a variant of the Diffie-Hellman scheme in which the number of bits exchanged is one-third of what is used in the classical Diffie-Hellman scheme, while the offered security against attacks known today is the same. Brouwer further discloses applications for this variant and conjecture an extension of this variant further reducing the size of sent information.

LIDL

Lidl discloses mapping from a finite extension F of the finite field K as a vector space over K.

PRESENTLY CLAIMED INVENTION

Independent claims 25, 33, 41, and 49, as presently claimed, recite a method, system, and article of manufacture of determining a public key having an optionally reduced length and a number p for a cryptosystem resident in a device that includes a memory. The method uses GF(p) or GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6). The method selects p, q, and g so that $p^2 - p + 1$ is an integer multiple of q and g of order q,

48807 v1

Application Serial Number: 09/498,716
1.111 Amendment dated March 10, 2004
Reply to Office Action dated December 10, 2003

Attorney Docket Number: 0225-4188

where g and its conjugates can be represented by B, where $F_g(X) = X^3 - BX^2 + B^p X - 1$ and the roots are g, g^{p-1}, g^{-p}. The method represents the powers of the conjugates of g using their trace over the field $GF(p^2)$ and computes the public key as a function of p, q, and B.

ElGamal discloses a public key system in $GF(p)$ and suggests that the public key system can be easily extended to any $GF(p^m)$, but states that "recent progress in computing discrete logarithms over $GF(p^m)$ where m is large makes the <u>key size required very large</u> for the system to be secure". ElGamal further states that "estimates for the running time for the fields $GF(p^m)$ with a small m seem better at the present time ... [and] it seems that it is better to use $GF(p^m)$ with $m = 3$ or 4 for implementing a cryptographic system." Thus, ElGamal teaches that it is <u>not feasible</u> to compute discrete logarithms <u>to achieve $GF(p^6)$ security</u>.

In contrast, claims 25, 33, 41, and 49, as presently claimed, recite the use of $GF(p)$ or $GF(p^2)$ arithmetic to achieve $GF(p^6)$ security, without explicitly constructing $GF(p^6)$. Furthermore, as the Examiner admits, ElGamal "does not disclose the conjugates and roots in such a case, or the order of the trace field employed". Thus, ElGamal not only <u>does not teach</u> representing the powers of the conjugates of g using their trace over the field $GF(p^2)$, but also <u>teaches away</u> from the presently claimed use of $GF(p)$ or $GF(p^2)$ arithmetic to achieve $GF(p^6)$ security.

The Examiner relies upon Brouwer and Lidl to make up for the shortcomings of ElGamal. Brouwer discloses a variant of the Diffie-Hellman scheme, but <u>does not</u> disclose a public key system in $GF(p)$ that can be extended to any $GF(p^m)$ and still achieve $GF(p^6)$ security. Similarly, Lidl discloses mapping from a finite extension F of the finite field K as a vector space over K, but also <u>does not</u> disclose a public key system in $GF(p)$ that can be extended to any $GF(p^m)$ and still achieve $GF(p^6)$ security. Thus, Brouwer and Lidl, either alone or taken in

48807 v1

Application Serial Number: 09/498,716
1.111 Amendment dated March 10, 2004
Reply to Office Action dated December 10, 2003

Attorney Docket Number: 0225-4188

combination, do not account for the shortcomings of ElGamal.

For the reasons stated above, ElGamal, Brouwer, and Lidl, alone or taken in combination do not teach or suggest the Applicants presently claimed method of determining a public key having an optionally reduced length and a number p for a cryptosystem resident in a device that includes a memory. Thus, the Applicants respectfully submit that the Examiner should withdraw these rejections as to independent claims 25, 33, 41, and 49.

Claims 26–32, 34–40, 42–48, and 50–56 depend from independent claim 25, 33, 41, or 49. For the previously stated reasons, independent claims 25, 33, 41, and 49 are allowable. Since any claim that depends from an allowable independent claim is also allowable, the Applicants also believe that the Examiner should withdraw these rejections as to dependent claims 26–32, 34–40, 42–48, and 50–56.
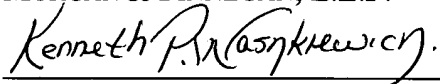
48807 v1

Application Serial Number: 09/498,716
1.111 Amendment dated March 10, 2004
Reply to Office Action dated December 10, 2003

Attorney Docket Number: 0225-4188

AUTHORIZATION

The Commissioner is hereby authorized to charge any additional fees which may be required for timely consideration of this Amendment under 37 C.F.R. §§ 1.16 and 1.17, including any extension of time, or credit any overpayment to Deposit Account Number 13-4500, Order Number 0225-4188.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Kenneth P. Waszkiewicz

Kenneth P. Waszkiewicz
Registration Number: 45,724

SENDER'S ADDRESS:
  MORGAN & FINNEGAN, L.L.P.
  345 Park Avenue
  New York, NY 10154-0053

  202-857-7887 – phone
  202-857-7929 – fax

Dated: March 10, 2004

48807 v1